

# ISO/IEC 20008-3:2024-12 (E)

## Information security - Anonymous digital signatures - Part 3: Mechanisms using multiple public keys

---

<b>Contents</b>		<b>Page</b>
Foreword .....		v
Introduction .....		vi
1	Scope .....	1
2	Normative references .....	1
3	Terms and definitions .....	2
4	Symbols and abbreviated terms .....	2
5	General model and requirements .....	3
5.1	General .....	3
5.2	Model .....	3
5.3	Requirements .....	4
6	Mechanisms without special capability .....	4
6.1	General .....	4
6.2	Mechanism 1 .....	5
6.2.1	Symbols .....	5
6.2.2	Key generation process .....	5
6.2.3	Ring signature process .....	5
6.2.4	Ring signature verification process .....	6
6.3	Mechanism 2 .....	6
6.3.1	Symbols .....	6
6.3.2	Key generation process .....	7
6.3.3	Ring signature process .....	7
6.3.4	Ring signature verification process .....	7
6.4	Mechanism 3 .....	8
6.4.1	Symbols .....	8
6.4.2	Key generation process .....	8
6.4.3	Ring signature process .....	8
6.4.4	Ring signature verification process .....	8
7	Mechanisms with linking capability .....	9
7.1	General .....	9
7.2	Mechanism 1 .....	9
7.2.1	Symbols .....	9
7.2.2	Key generation process .....	10
7.2.3	Ring signature process .....	10
7.2.4	Ring signature verification process .....	10
7.2.5	Ring signature linking process .....	11
7.2.6	Event-linkable type .....	11
8	Mechanisms with tracing capability .....	11
8.1	General .....	11
8.2	Mechanism 1 .....	11
8.2.1	Symbols .....	11
8.2.2	Key generation process .....	11
8.2.3	Ring signature process .....	12

8.2.4	Ring signature verification process .....	12
8.2.5	Ring signature tracing process .....	13
9	Mechanisms with threshold capability .....	13
9.1	General .....	13
9.2	Mechanism 1 .....	13
9.2.1	Symbols .....	13
9.2.2	Key generation process .....	13
9.2.3	Ring signature process .....	13
9.2.4	Ring signature verification process .....	14
9.3	Mechanism 2 .....	14
9.3.1	Symbols .....	14
9.3.2	Key generation process .....	14
9.3.3	Ring signature process .....	15
9.3.4	Ring signature verification process .....	15
Annex A (normative)	Object identifiers .....	16
Annex B (normative)	Conversion functions .....	17
Annex C (informative)	Numerical examples of mechanisms in this document .....	18
Bibliography	.....	23